Disclosure AUS8-2003-0692

Prepared for and/or by an IBM Attorney - IBM Confidential

Created By Joseph V Lampitt On

Required fields are marked with the asterisk (*) and must be filled in to complete the form .

***Title of disclosure (in English)**

Efficient, Scalable, Integrated Method for Modifying DHCP Servers

Summary

Status		
Final Deadline		
Final Deadline Reason		
*Processing Location		
*Functional Area	select	
Attorney/Patent Profess		
IDT Team	select	

Submitted Date	04/17/2003 08:36:51 AM MDT	
*Owning Division	select	
Incentive Program		
Lab		
*Technology Code		

PVT Score

Inventors with a Blue Pages entry

Inventors: Joseph V Lampitt/Austin/IBM, Paul B Finley/Austin/IBM, Scott Tran/Austin/IBM

Inventor Name	Inventor Serial	Div/Dept	Inventor Phone	Manager Name
> Lampitt, Joseph V. (Joe)		7T/B9RS		
Finley, Paul B.		7T/B9RS		
Tran, Vi T. (Scott)		7T/B9RS		

> denotes primary contact

Inventors without a Blue Pages entry

IDT Selection

Attorney/Patent Professional	Marilyn Dawkins/Austin/IBM
IDT Team	Gerald McBrearty/Austin/IBM Kenneth Banning/Austin/IBM Johnny Shieh/Austin/IBM Thomas Weaver/Austin/IBM Kim Tran/Austin/IBM Deanna Brown/Austin/IBM Dwip N Banerjee/Austin/IBM Faisal Awada/Austin/IBM Jeanne Sparlin/Austin/IBM Trey Ramsay/Austin/IBM Mark Hamzy/Austin/IBM Steve Pratt/Austin/IBM Wei Kuo/Austin/IBM Rafael Cabezas/Austin/IBM Vinit Jain/Austin/IBM Andrew Dunshea/Austin/IBM Susann Keohane/Austin/IBM Vasu Vallabhaneni/Austin/IBM Luc Smolders/Austin/IBM Vasu Vallabhaneni/Austin/IBM@IBMUS Luc Smolders/Austin/IBM@IBMUS Fernando Sanchez/Austin/IBM Terry Thomas/Austin/IBM Michael Panico/Austin/IBM Luke Browning/Austin/IBM James Moody/Austin/IBM Stephen M Tee/Austin/IBM Corradino Jones/Austin/IBM
Response Due to IP&L	05/17/2003

***Main Idea**

To view the main idea for this disclosure, click on this doclink --->[ ] **(If you are prompted to enter a server name, please enter D01DB068/01/A/IBM)**

***Patent Value Tool**

* **1.** Select the single most appropriate technology category for your invention from the following technologies list.

Main Idea for Disclosure AUS8-2003-0692

Prepared for and/or by an IBM Attorney - IBM Confidential

Archived On 06/21/2003 12:04:04 AM

Title of disclosure (in English)
Efficient, Scalable, Integrated Method for Modifying DHCP Servers

Main Idea of disclosure
1. Background: What is the problem solved by your invention? Describe known solutions to this problem (if any). What are the drawbacks of such known solutions, or why is an additional solution required? Cite any relevant technical documents or references.
Currently, a DHCP server does not allow requests from machines to modify another machine's DHCP configuration. For example, machine A cannot request that the lease time be extended for machine B. However, there are several instances where this is desireable.

First, an installation server (in this case, a seperate machine from the DHCP server) needs to network install another machine that is a DHCP client. For the installation to succeed, the client's lease time must be increased so that the lease does not expire during the installation and the client's bootfile must be specified along with the boot server. One way to solve this problem is to have the installation server run a remote command, like rsh, to modify the DHCP configuration file and restart the DHCP daemon.

This solution has the following problems. First, the administrator is required to setup another service to allow remote clients to execute commands, such as rsh or ssh. However, with rsh or ssh access, the remote clients will be able to modify more than just the configuration of the DHCP service. Second, there is no locking mechanism to prevent two operations from modifying the configuration file. Third, the dhcp daemon must be restarted.

Another solution is to have one machine be both the DHCP server and the installation server. This would allow the installation service to execute local commands that modify the DHCP service configuration but restricts the user to having both the installation and DHCP service on one machine. What if the user wanted to have mutiple installation servers for various operating systems and only one DHCP server?

There are several other scenarios where allowing remote machines to modify a DHCP server is desireable. One scenario is a DNS server needs to update the hostname assigned to a specific MAC address in the DHCP configuration file. Another scenario is a machine managing printers needs to update the list of known printers for a specific subnet or class of DHCP clients. One more scenario is a machine that manages various network services needs to update the DHCP options on the server.

2. Summary of Invention: Briefly describe the core idea of your invention (saving the details for questions #3 below). Describe the advantage(s) of using your invention instead of the known solutions described above.
The invention is to extend the DHCP protocol to accept "modify" packets from registered systems. First, a system needing to modify options for DHCP clients would register with the DHCP server. Registering could be as simple as placing a trusted key on the DHCP server for the registering system. The trusted key could be used to verify that the system sending a "modify" packet has modification priveleges. Or verification could be based upon the IP address and MAC address of the requesting system, similar to how rsh authenticates based upon hostname and user. While some form of authentication must occur, how the authentication is implemented is unimportant since one of several known methods could be used. Once a system is registered with the DHCP server, the registered system can send "modify" packets to the DHCP server.

The invention provides the following advantages to current solutions. Systems needing to modify DHCP

parameters can do so without relying on other protocols or services. Registered systems will only be able to modify the DHCP service, since the DHCP daemon receives the packet and authenticates the requestor. Control of the DHCP service is decoupled from the system running the DHCP server since multiple machines performing different functions can update the DHCP service.

3. Description: Describe how your invention works, and how it could be implemented, using text, diagrams and flow charts as appropriate.
First, a system needing DHCP modification priveleges registers with the DHCP server using a known authentication method. Now the system can send "modify" packets to the DHCP server.
The modification packet will be similar to the following:
IP Header
TCP Header
DHCP Message

message type = code for DHCPMODIFY (i.e. "9")
other standard parameters for a DHCP message
client/class/network = DHCP client, class, or network to modify
option = name of option to be modified plus value

Depending on the type of authentication used, the client and option parts of the message may be encrypted. Now the DHCP service handles the message and ensures that the server sending the DHCPMODIFY packet has modificaiton priveleges. Then the DHCP service modifies the stored configuration information for the specified client, class, or network. Once the information has been modified the server sends a new DHCPACCEPT packeting indicating the changes were successfully made. Now any new DHCP requests will receive the updated information.

This section illustrates an example of how an installation server would modify the lease-time of a client. First, the administrator registers the installation server based upon the desired authentication method. If authentication involves the IP address and MAC address of the installation server, then these values would be stored securely on the DHCP server. Now, the installation server needs to increase the lease-time to 10800 seconds for "client1" and sends a DHCP packet to the DHCP server with the following data:

message type = DHCPMODIFY code
other standard DHCP parameters
client = client1
option = 51 (lease-time)
option value = 10800

Next, the DHCP server handles the request, modifies the stored configuration information for the client, and sends back a DHCPACCEPT packet indicating the request was successful. If the request fails, the DHCP server would send a DHCPDECLINE message.